UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Alexander Medvinsky, et al.	GROUP ART UNIT:	2135
APPLN. NO.:	09/890,180	EXAMINER:	To, Baotran N.
FILED:	January 24, 2002	Confirmation No.:	7559
TITLE:	**KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S**		

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

In response to the Final Office Action mailed from the U.S. Patent and Trademark Office on November 19, 2010, Applicants request review of the final rejection in the above-identified application. This request is being filed with a Notice of Appeal and authorization for the required fee. An extension of time is hereby requested, and this response is accompanied by authorization for the fee required under 37 C.F.R. 1.136(a). No other fees are believed to be due; however, the Commissioner is hereby authorized to charge any additional fees which may be required at any time during the prosecution of this application without specific authorization, or credit any overpayment, to Deposit Account No. 505278.

No amendments are being filed with this request. The review is requested for the reasons stated in the remarks below.

Status of Claims

Claims 1-19 are pending. Of these, claims 1, 6, 7, 11, and 15 are the independent claims.

Claim Rejections – 35 U.S.C. § 103(a)

Claims 1-19 stand finally rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Barkan, European Patent Application Number 0 738 058 (hereinafter "Barkan"), in view of Ganesan, U.S. Patent Number 5,838,792 (hereinafter "Ganesan"). The Applicants respectfully traverse.

The Barkan reference describes an apparatus for transferring an encryption key in a secure way to facilitate establishing a secure communication link. The Barkan apparatus includes a key management device attached to each user's encryption machine. The key management device contains a list of secure communication partners and their respective encryption keys and parameters. To initiate a secure link session, the user keys-in the identification of the desired addressee. If the details of the addressee are available, the Barkan apparatus automatically transfers the encryption key and the other communication parameters for the addressee to the encryption machine to establish the secure link. If the details of the addressee are not available, the Barkan apparatus automatically connects to a secure key distribution center to get the encryption key and parameters for that addressee. After establishing the secure link session between a first user's encryption machine and a second user's encryption machine, Barkan describes a communication path that is from the first user's encryption machine (element 21), through a communication channel (element 213) for the first user (facility 1), through a communication channel (element 233) for the second user (facility 3), and to the second user's encryption machine (element 23). Thus, the established secure link session in Barkan is a direct communication path from the first user's encryption machine to the second user's encryption machine.

In contrast, the presently claimed invention, as recited in independent claims 1, 6, 7, and 15, describes a method and system for "establishing a secure communication channel in an IP telephony network … wherein call signaling messages between the first telephony adapter and the second telephony adapter are routed through the first gateway controller and the second gateway controller, and encrypted messages are exchanged between the first telephony adapter and the second telephony adapter on the secure communication channel." A first user is coupled to a first telephony adapter, which is coupled to a first gateway controller. Similarly, a second user is coupled to a second

telephony adapter, which is coupled to a second gateway controller. The first gateway controller and the second gateway controller connect to and control user access to the IP telephony network. The path of the communications between the first user and the second user is from the first telephony adapter, then to the first gateway controller, then to the IP telephony network, then to the second gateway controller, and then to the second telephony adapter.

The Barkan and Ganesan references do not describe a communications path for call signaling messages from the first telephony adapter to the second telephony adapter that is **routed through the first gateway controller and the second gateway controller**, as recited in Applicant's independent claims.

Applicant teaches that there is a communications path for call signaling messages, and a different communications path for encrypted messages. Applicant's communications path for **call signaling messages** from the first telephony adapter to the second telephony adapter is routed through the first gateway controller and the second gateway controller. Applicant's communications path for **encrypted messages** is different, in that encrypted messages are exchanged between the first telephony adapter and the second telephony adapter on the secure communication channel.

The communications path described in Barkan utilizes a wired or wireless communication means on the standard communication channel (element 213) as a direct connection between the first user's encryption machine (facility 1) and the second user's encryption machine (facility 3). Ganesan does not make up for this additional shortcoming of Barkan because it does not describe a communication path for call signaling messages from the first telephony adapter to the second telephony adapter that is routed through the first and second gateway controllers, as described in Applicant's independent claims.

Thus, the Barkan and Ganesan references, taken either alone or in combination, do not describe a communications path for call signaling messages from the first telephony adapter to the second telephony adapter that is routed through the first and second gateway controllers.

In addition, it appears that the Examiner's arguments are substantially based on incorrectly equating the gateway controllers of Applicant's claims, which are used for call signaling messages, to Barkan's key distribution centers.

The term "gateway controller" or "media gateway controller" has long been known to persons having ordinary skill in the art; for example, http://tools.ietf.org/html/draft-cuervo-navdec-mg-arch-00 (dated November 1998) describes exemplary functions of a media gateway controller. The final Office Action appears to equate the key distribution centers of Barkan with Applicants' gateway controllers; however, a key distribution center is not a gateway controller. A primary function of a gateway controller is call signaling – e.g., it forwards call signaling messages between telephony adapters and also includes an encryption key in those signaling messages. Applicant teaches, in an exemplary embodiment, that keys are exchanged via first and second gateway controllers that are used for call signaling, where keys are included in the VoIP call signaling/call setup.

In contrast to Applicants' claimed gateway controller, the key distribution center disclosed by Barkan is generally for keeping track of encryption keys. For example, Figure 1 of Barkan shows that keys can be exchanged through Key Distribution Centers, where a function of a Key Distribution Center is merely key management, not VoIP call signaling. Although Barkan, at col. 14, lines 11-15, does say that some implementations can use the same channel for key exchange and call signaling, this statement is immediately followed (at col. 14, lines 16-24) by clearly identifying Barkan's communication channel as physical lines that can be, e.g., wireless links, dialup connection, etc. Barkan fails to disclose or suggest the possibility of key exchange and call signaling to occur over the same protocol. A Key Distribution Center in Barkan is described as issuing device certificates and is not disclosed as being involved in VoIP call signaling. Thus, in the Barkan invention, key exchanges do not occur in the same protocol as call signaling.

Since Ganesan fails to supply features missing from Barkan, the combination of Barkan and Ganesan cannot suggest the presently claimed invention and cannot render the claims obvious. Thus, no matter how Barkan and Ganesan may be combined (even assuming, *arguendo*, that one of ordinary skill in the art would be led to combine them)

the resulting combination is not the invention recited in independent claims 1, 6, 7, 11, and 15.

For at least the aforementioned reasons, independent claims 1, 6, 7, 11, and 15 are patentable over the Barkan and Ganesan references, either taken alone or in combination. Thus, the Examiner should withdraw the 35 U.S.C. § 103 obviousness rejection as to independent claims 1, 6, 7, 11, and 15.

Claims 2-5, 8-10, 12-14, and 16-19 depend from either independent claim 1, 6, 7, 11, or 15. For the previously stated reasons, independent claims 1, 6, 7, 11, and 15 are allowable. Since any claim that depends from an allowable independent claim is also allowable, the Applicants respectfully submit that the Examiner should also withdraw this rejection as to dependent claims 2-5, 8-10, 12-14, and 16-19.

Conclusion

Claims not specifically mentioned above are allowable at least due to their dependence on an allowable base claim.

In light of the arguments presented above, it is respectfully submitted that all pending claims are in condition for allowance. Reconsideration and withdrawal of the final rejection of the claimed invention is respectfully requested.

Respectfully submitted,
ALEXANDER MEDVINSKY, et al.

Date: May 19, 2011

BY: /Stewart M. Wiener/
Stewart M. Wiener
Registration No. 46,201
Attorney for Applicants

Motorola Mobility, Inc.
101 Tournament Drive
Horsham, PA 19044
Telephone: (215) 323-1811
Fax: (215) 323-1300